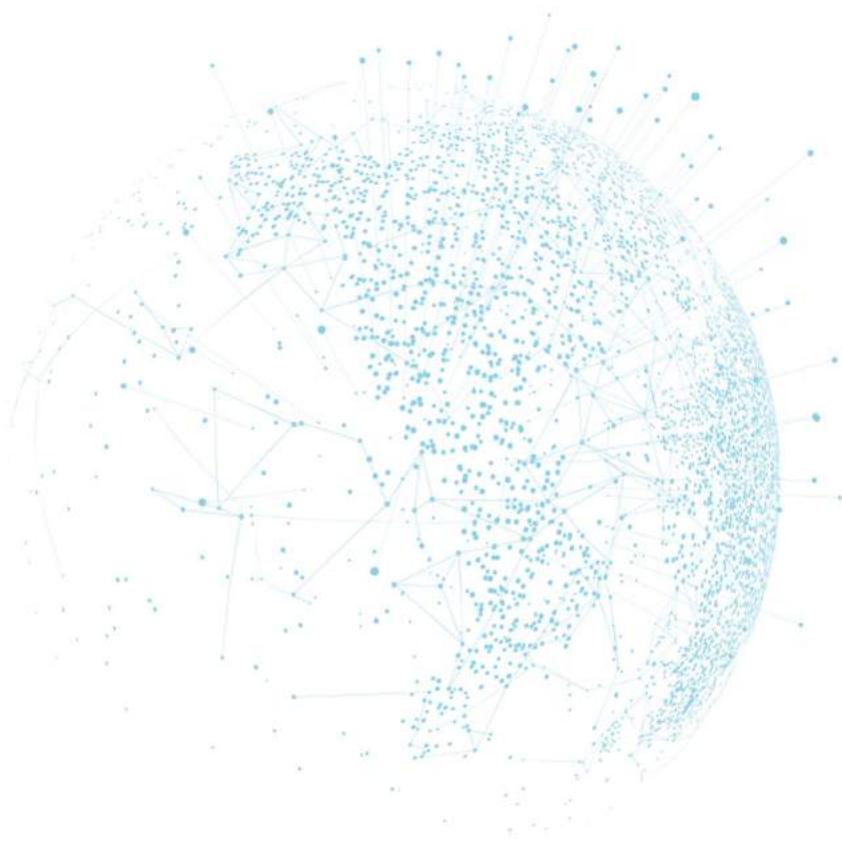




可信区块链推进计划  
TRUSTED BLOCKCHAIN INITIATIVES

# 区块链司法存证应用白皮书

(1.0 版)



可信区块链推进计划  
2019年6月



---

## 版 权 声 明

---

本白皮书版权属于可信区块链推进计划，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：可信区块链推进计划”。违反上述声明者，将追究其相关法律责任。

# 《区块链司法存证应用白皮书》编写委员会

**指导单位：**最高人民法院信息中心

**牵头单位：**中国信息通信研究院、上海高级人民法院

**参与单位：**吉林省高级人民法院、江西省高级人民法院、山东省高级人民法院、四川省高级人民法院、广西壮族自治区高级人民法院、天津市高级人民法院、北京互联网法院、杭州互联网法院、广州互联网法院、徐州市公安局、中国司法大数据研究院、上海金桥信息股份有限公司、北京泛融科技有限公司、北京中经天平科技有限公司、杭州秘猿科技有限公司、腾讯科技（深圳）有限公司、浙江蚂蚁小微金融服务集团股份有限公司、西安纸贵互联网科技有限公司、北京华宇软件股份有限公司、京东数字科技控股有限公司、深圳法大大网络科技有限公司、江苏中兴华易科技发展有限公司、重庆市公证协会、百度在线网络技术（北京）有限公司、北京优炫软件股份有限公司

**编写组：**何宝宏、曹红星、魏凯、杨白雪、纽加强、卢兴亚、王珩、张宏庆、吴斌、王晋军、柳畅、钱靖、蒋鸿铭、蔡弋戈、徐惠、刘雅冬、米坤、周晓健、齐宁宁、李琳、易君召、袁野、肖伟、赵春学

**专家组：**陈奇伟、张立华、任拔、匡华、杨崇华、杨海云、冯炳南、黄靖淞、姚海涛、沈洪、姚俊、陈含新、陈炳陶、魏磊、薛新伟、张保川、董兵兵、崔斌、张仁叶、张丰程

## 前 言

随着信息化的快速推进，诉讼中的大量证据以电子数据存证的形式呈现，电子证据在司法实践中的具体表现形式日益多样化，电子数据存证的使用频次和数据量都显著增长。不同类型电子证据的形成方式不同，但是普遍具有易消亡、易篡改、技术依赖性强等特点，与传统实物证据相比，电子证据的真实性、合法性、关联性的司法审查认定难度更大。

传统的存证方式面对日益增长的电子数据存证需求，逐渐显露出成本高、效率低、采信困难等不足。此外，在司法实践中，当事人普遍欠缺举证能力，向法院提交的电子证据质量较差，存在大量取证程序不当、证据不完整、对案件事实指向性差等问题，直接影响到电子证据在诉讼中的采信比例。

区块链技术特有的不可篡改、不可抵赖、多方参与等特性，与电子数据存证的需求天然契合。电子数据存证是潜在的区块链技术重要应用落地领域。区块链与电子数据存证的结合，可以降低电子数据存证成本，方便电子数据的证据认定，提高司法存证领域的诉讼效率。

本白皮书由浅及深地介绍了区块链电子数据存证的特点和系统设计原则。从电子数据存证的发展现状入手，阐释了区块链电子数据存证对证据三性认定的关系，点明了区块链与电子数据存证的结

合点和重要意义，并为区块链存证系统总体设计和关键技术进行了表述和总结。最后，本白皮书还分享了几个区块链司法存证业务领域和实际案例，为区块链应用的开发和创新提供多视角的思路。

# 目 录

一、电子数据存证背景.....	1
（一）概述 .....	1
（二） 电子数据存证的现状.....	2
（三） 电子数据存证法律依据.....	3
（四） 电子数据存证在司法实践中存在的问题.....	6
二、基于区块链的电子数据存证.....	9
（一） 区块链存证系统的关键技术.....	10
（二） 区块链电子数据存证在司法实践中的应用价值.....	14
三、区块链存证提高电子证据认定效率.....	17
（一） 电子数据真实性认定的要素 .....	17
（二） 电子数据关联性和合法性的认定要素 .....	22
（三） 区块链存证系统对电子数据认定的作用 .....	23
四、区块链存证系统的参考架构.....	27
（一） 区块链存证系统的技术要求 .....	27
（二） 区块链存证系统的参考架构 .....	30
五、区块链电子数据存证的应用场景.....	33
（一） 法院行业应用.....	33
（二） 司法协同应用.....	36
（三） 社会存证应用.....	36
六、区块链司法存证存在的挑战.....	40
（一） 法务与技术的对接不畅 .....	41
（二） 司法业务模式有待优化 .....	42
（三） 民众接受程度有待提高 .....	42
七、结论.....	43
（一） 电子数据发展带来了挑战 .....	43
（二） 区块链提升电子数据认定效率 .....	43
（三） 多参与方互通合作，完善标准推广应用 .....	44
参考文献： .....	46
附件： 参考应用案例.....	47
吉林省高级人民法院电子证据平台 .....	47

山东省高级人民法院电子证据平台 .....	47
北京互联网法院“天平链”电子证据平台 .....	48
杭州互联网法院“司法区块链” .....	48
广州互联网法院“网通法链” .....	49
郑州市中级人民法院电子证据平台 .....	49
成都市郫都区人民法院电子证据平台 .....	50

## 一、电子数据存证背景

### （一）概述

随着社会跨入数字化时代，数字化已广泛渗透到社会生活的方方面面。截至 2018 年 12 月，中国网民的规模达到了 8.29 亿，较 2017 年提升了 3.8%；其中手机网民的规模达到了 8.17 亿；即时通信用户规模达 7.92 亿。<sup>1</sup>2018 年我国数字经济总量达到 31.3 万亿元，占 GDP 比重超过三分之一，达到 34.8%，占比同比提升 1.9 个百分点。<sup>2</sup>数字化在政治、经济、思想文化和社会生活等诸多方面深刻影响和重塑着社会发展方式和社会治理格局。

2019 年 3 月 12 日上午，第十三届全国人民代表大会第二次会议在人民大会堂举行第三次全体会议，最高人民法院院长周强做最高人民法院工作报告时明确表示要“推进司法改革与现代科技深度融合”。在数字化的浪潮下，在科技进步的支持下，司法和正义普惠化更容易实现，科技对于司法的作用和价值正不断提高，司法科技已是势在必行。

随着数字化发展，电子证据在世界各国的司法证明活动中的作用日益突出，电子证据已成为证据体系中不可忽视的重要部分，社会开始步入“电子证据时代”。相对于物证时代的“科学证据”而言，电子证据的科技含量无论在广度还是深度上，都大大超出了一般物证的水平。电子证据在我国立法中取得合法地位之后，开始大规模

---

<sup>1</sup> 第 43 次《中国互联网络发展状况统计报告》

<sup>2</sup> 中国信息通信研究院，《中国数字经济发展白皮书》



地正式介入案件，在越来越多的案件中发挥着前所未有的作用。

## （二） 电子数据存证的现状

移动互联网的普及带来了大量电子数据存取证的需求。截止2018年12月，我国网络新闻用户规模达6.75亿，网络购物用户规模达6.10亿，网上外卖用户规模达4.06亿，网络支付用户规模达6.00亿，网络视频用户规模达6.12亿，短视频用户规模达6.48亿。随着微博、微信等网络通讯工具的高度普及适用，电子数据存证，已成为现今社会的实际情况要求。

电子证据在确立了其作为独立证据的地位后得到快速发展。2012年《中华人民共和国民事诉讼法解释》中，明确了适用电子数据的规定。<sup>3</sup> 2018年，人民法院新收知识产权民事、行政和刑事案件数量达到334951件，比2017年增加97709件，同比上升41.19%。其中，知识产权行政一审案件和民事一审案件呈大幅上升态势，增幅分别达到53.57%和40.97%。<sup>4</sup> 据中国裁判文书网数据，近3年约5000份知识产权民事判决书进行统计，约89%的案件使用了电子证据。<sup>5</sup>

《2018年中国电子证据应用白皮书》中数据显示，电子证据被认定为法律事实的案件越来越多，涉案保全金额年增长达15%。全国民事案件超73%涉及电子证据。电子证据被应用于各种商务往来，离婚财产、证券纠纷、互联网金融、电子病历，聊天记录中等不同类

---

<sup>3</sup> <最高人民法院关于适用《中华人民共和国民事诉讼法》的解释>第116条第二款

<sup>4</sup> 数据来源：中国司法大数据研究院

<sup>5</sup> 李自柱，“知识产权诉讼中有关电子证据的两个问题”，《电子知识产权》2016年第12期。

型的场景高达 43 种。

### （三） 电子数据存证法律依据

#### 1. 诉讼法及司法解释

2012 年之前，在我国法律体系下，电子数据不能作为独立证据参与诉讼。我国 2012 年修改的《中华人民共和国民事诉讼法》《中华人民共和国刑事诉讼法》以及 2014 年修改的《中华人民共和国行政诉讼法》分别在第 63 条、第 48 条、第 33 条将电子数据作为一种新的证据种类纳入立法，使其获得了独立的证据地位。2015 年《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第 116 条第二款规定了电子数据的部分形式。2019 年公安部发布《公安机关办理刑事案件电子数据取证规则》，其中第 7 条规定了电子数据提取的方式方法<sup>6</sup>。2011 年国家工商总局发布了工商市字〔2011〕248 号《关于工商行政管理机关电子数据证据取证工作的指导意见》，在其三、四、五条就电子数据证据取证的方式和条件进行了规定。

上述法条和司法解释明确了电子证据在司法实践中可以作为独立证据，并对电子数据的取证手段进行了一些规定。其规定的取证手段包含：1. 扣押、封存原始存储介质；2. 现场提取电子数据；3. 网络在线提取电子数据；4. 冻结电子数据；5. 调取电子数据；<sup>7</sup>6. 书式固定；7. 拍照摄像；8. 拷贝复制；9. 委托分析。<sup>8</sup> 其中扣押电子数

<sup>6</sup> <http://www.mps.gov.cn/n2254314/n2254409/n4904353/c6337154/content.html>

<sup>7</sup> 《公安机关办理刑事案件电子数据取证规则》

<sup>8</sup> 《关于工商行政管理机关电子数据证据取证工作的指导意见》

据原始载体是首位选择。

## 2. 《电子签名法》

《电子签名法》第 5 条明确了满足法律要求电子数据原件的形式。第 8 条阐述了审查数据电文真实性应对考虑的因素。

第五条“符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

- （一）能够有效地表现所载内容并可供随时调取查用；
- （二）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。”

第八条“审查数据电文作为证据的真实性，应当考虑以下因素：

- （一）生成、储存或者传递数据电文方法的可靠性；
- （二）保持内容完整性方法的可靠性；
- （三）用以鉴别发件人方法的可靠性；
- （四）其他相关因素。”

## 3. 公证体系法律法规和行业规范

关于电子证据保全公证的操作程序，主要散见于《公证法》、《公证程序规则》、中国公证协会发布的《关于办理保全证据公证的指导意见》、《办理保全互联网电子证据公证的指导意见》等。

综合上述法律法规及行业规范的规定，电子证据的保全公证的基本程序包含以下要点：应当使用公证机构的计算机进行；由公证

员按照申请人提供的书面操作程序进行操作；公证员应当按照顺序记录登录网络、进入网址、下载、打印（或刻录）等整个证据保全过程和所使用的操作软件名词、版本；公证员审核下载内容与网页内容是否相符；制作电子证据保全公证书；在公证申请人主动提出或者保全的电子数据具有复杂性、重要性时，公证员应当对保全的过程进行录像，并将录像资料与电子证据保全资料一并封存。电子证据保全的方式主要包括：备份、打印（按照书证方式）、拷贝、拍摄。对于当事人无法确切证明电子邮件或聊天记录中对方身份的，保全的电子数据可能不具有证据效力。

由此看出，电子数据公证的流程较繁琐，证据保全方式成本较高，对当事人的举证能力有一定要求。

#### 4. 《最高人民法院关于互联网法院审理案件若干问题的规定》

最高人民法院在 2018 年 9 月 7 日印发的《关于互联网法院审理案件若干问题的规定》，第十一条“当事人对电子数据真实性提出异议的，互联网法院应当结合质证情况，审查判断电子数据生成、收集、存储、传输过程的真实性，并着重审查以下内容：（一）电子数据生成、收集、存储、传输所依赖的计算机系统等硬件、软件环境是否安全、可靠；（二）电子数据的生成主体和时间是否明确，表现内容是否清晰、客观、准确；（三）电子数据的存储、保管介质是否明确，保管方式和手段是否妥当；（四）电子数据提取和固定的主体、

工具和方式是否可靠，提取过程是否可以重现；（五）电子数据的内容是否存在增加、删除、修改及不完整等情形；（六）电子数据是否可以通过特定形式得到验证。当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。”

《规定》首次承认了经区块链存证的电子数据可以用在互联网案件举证中，标志着我国区块链存证技术手段得到司法解释认可。

#### **（四） 电子数据存证在司法实践中存在的问题**

虽然在法条、司法解释和相关规定中，对电子证据的范畴、原件形式、取证手段等做了一些规定，但电子证据在司法实践中包括存证环节、取证环节、示证环节、举证责任和证据认定中依然存在痛点。

##### **1. 存证中的问题**

电子数据具有数据量大、实时性强、依赖电子介质、易篡改、易丢失等特性，在存证中面临一些问题。

##### **（1） 单方存证**

传统的存证方式有公证存证、第三方存证、本地存证等，这些方式本质上都是由一方控制存证内容，是中心化的存证方式。中心化存证下，一旦中心遭受攻击，容易造成存证数据丢失或被篡改。

##### **（2） 存储成本高**

电子数据依赖电子介质存储，为了存储安全，经常需要使用多备份等方式，加之电子介质有其使用寿命，因此存储成本较高。

## 2. 取证中的问题

### （1）证据原件与设备不可分

目前，在对某些本地产生的电子数据进行取证时，原件只能留存在产生电子数据的设备当中，证据原件和设备是不可分的。证据原件一旦要离开设备，就变成了复制品而不能成为定案依据。因此，在民事诉讼中，经常发现当事人需要向法院展示手机等设备，迫使当事人本人必须到庭参加进行操作；在刑事调查和行政调查中，因查封电子数据原始载体是取证的首要手段，被调查人的电脑硬盘、服务器可能被全部拿走而进行调查，导致被调查人正常业务被迫停止的情况。

这一情况给司法相对人造成了不必要的麻烦，事实上也很难杜绝当事人此前已经对原始文件进行的删改，是事倍功半的。

### （2）原件可以被单方修改

在目前的互联网软件上形成的数据原件，都是基于当事人在互联网软件服务商处注册的用户名密码下行为所致。在这种数据逻辑结构下，也基于对隐私权的保护，当事人对自己数据的删改，包括对其删改记录的删改是其当然的权限。那么，所谓的原件到底是不是事件发生时真实、原始和完整的数据，互联网软件服务商也无法给出确切的答案。即使互联网软件服务商给出了他所留存的数据，

也无法证明这个数据是否经过了互联网软件服务商的删改，不能完全保证相关数据的真实性；严格来讲，相关数据只能作为线索和间接证据使用。

因此，在对电子数据取证的时候，所取证据是否属于原件，也是存疑的。

### 3. 示证中的问题

电子数据展示和固定是电子数据使用的重要环节，由于电子数据的存在形式是存储在电子硬件中的电子信息，要获取其内容需要使用相应的软件读取和展示。这给示证带来了困难，这表现在：

（1）并非所有电子数据的内容都可以通过纸质方式展示和固定，例如电子数据的电子签名信息和时间信息。

（2）对电子数据原件的截图、录像、纸质打印，复制存储都一般而言交由当事人自己完成，而其中的差异是难以在原件和复制件核对查验时充分验明的，这给了当事人篡改数据的空间。

（3）示证的困难使得对电子数据公证的需求增加，这严重加大了当事人的举证负担，也严重浪费了社会司法资源。

### 4. 举证中的问题

在诉讼中，双方都会提交自己留存的电子数据作为证据。在当事人分别控制自己的数据的情况下，非常容易发生双方提交的证据有出入，甚至是矛盾的情况。在没有其他佐证的情况下，证据的真实性认定非常困难，双方提交的电子数据都无法成为断案依据。在

这种无法判断案件事实的情况下，法官很可能需要依赖分配举证责任来进行断案。而一般的举证责任分配原则是谁主张，谁举证，无法举证则承担败诉的后果。那么在这种情况下，积极篡改自己数据的一方可以在这种举证责任的安排下获利。

## 5. 证据认定中的问题

一切证据“必须经过查证属实，才能作为定案的根据”，是在世界范围内具有普适性的最重要的司法原则之一。证据的认定，通常是认定证据“三性”的过程，即证据真实性、合法性和关联性。电子数据作为证据也需要经过“三性”判定。电子数据因为数据量大、数据实时性强、保存成本高、原件认定困难等原因，对证据的“三性”认定依然较困难，电子数据经常因为难以认定而无法对案件起到支撑作用，这对法官和当事人都造成了较大压力。

## 二、基于区块链的电子数据存证

区块链（Blockchain）是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术（Distributed Ledger Technology）。典型的区块链以块-链结构存储数据。作为一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式，区块链凭借其独有的信任建立机制，正在改变诸多行业的应用场景和运行规则，是未来发展数字经济、构建新型信任体系不可或缺的技术。



术之一。<sup>9</sup>

利用区块链及其扩展技术可以在电子数据的生成、收集、传输、存储的全生命周期中，对电子数据进行安全防护、防止篡改、并进行数据操作的审计留痕，从而为相关机构审查提供有效手段。

区块链特殊的存储方式进行电子数据存证，以无利害关系的技术作为第三方身份（技术和算法充当虚拟第三方），将需要存证的电子数据以交易的形式记录下来，打上时间戳，记录在区块中，从而完成存证的过程。在数据的存储过程中，多个参与方之间保持数据一致性，极大降低了数据丢失或被篡改的可能性。

## （一） 区块链存证系统的关键技术

区块链具有的适用于电子数据存证的能力，来源于区块链系统的关键技术，关键技术包括两方面：核心技术和相关技术。区块链的核心技术包括：共识机制、存储结构、通信方式等，用于保障区块链的多方参与、难篡改、难丢失的特性。区块链的相关技术包括：可信存储、电子身份、可信时间等，为区块链系统的多种应用场景提供支持。

### 1. 核心技术

#### （1）共识机制

共识算法用于协调区块链全网中各节点数据的一致性。共识算法通过制定达成共识的规则，实现节点选举、数据一致性验证和数

---

<sup>9</sup> 中国信息通信研究院《区块链白皮书（2018）》。

据同步控制等功能。一般来说共识算法具有如下功能：

- 1) 参与共识的节点在互不信任的条件下达成共识；
- 2) 支持节点独立进行算法运算，不依赖任何其他节点数据和状态；
- 3) 保证各节点对上链数据打包区块的计算能收敛并达到最终一致性；
- 4) 声明在一定规模的节点环境下达成共识所需的理论时间；
- 5) 应有明确的抗恶意攻击指标。

## (2) 签名验签

数字签名是使用非对称密钥加密技术与数字摘要技术，用于鉴别数字信息的方法。主要用于确定消息确实是由发送方签名并发出来，并确定接收到的消息的完整性，没有在传输过程中被篡改。

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用哈希函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

## (3) 链式存储结构

链式存储结构是将一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间先后顺序连接成链条的一种

数据结构。由于后一个区块中包含着前面区块的特征信息，因此如果想要修改其中一个区块中数据，需要将链式存储结构中的后序区块全部修改。而随着区块链中区块数量的不断增加，修改难度也不断增大。因此链式存储结构有效的提高了存储其中的数据的防篡改和防伪造能力。

#### (4) P2P 通讯

P2P（点对点）是指网络中的每个节点的地位都是对等的，每个节点既充当服务器，为其它节点提供服务，同时也享用其它节点提供的服务。P2P 网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，可以无需中间环节和服务器的介入，避免了可能的瓶颈，凸显了网络可扩展性、健壮性等方面的优势。

区块链中的各节点是典型的相互平等，不分主次的服务器网络，通过 P2P 通讯机制可以实现节点间数据就近快速同步的效果。同时也提高了整个区块链的抗网络攻击的能力。

## 2. 相关技术

#### (1) 电子身份认证

电子身份是一种数字化唯一身份标识，用于在 IT 系统中对人、组织、现实主体等进行唯一标注。电子身份认证使用各种验证手段来校验现实主体与电子身份间的合法对应关系，如带有智能芯片的身份卡、指纹、虹膜、语音等。电子身份认证的核心是数字签名技

术，它保证了用户身份的唯一性和合法性。

电子身份认证是司法存证主体及用户的反欺诈认证的基础，使用电子身份可以准确的记录行为方主体、操作人员信息，是电子数据有效性的基础保障。电子身份认证可以通过权威机构信息认证、大数据、人工智能方式对行为人的真实性进行验证，也可以直接在区块链上进行构建。

## （2）时间戳服务

时间戳是一个能够表示一份电子数据在一个特定时间点已经存在的完整的可验证的数据。主要提供一份电子证据，以证明某个电子数据的产生时间。在实际应用上，它可以使用在包括电子商务、金融活动的各个方面，尤其可以用来支撑公开密钥基础设施的“不可否认”服务。

可信时间戳是将电子数据摘要和权威时间源绑定，由国家授时中心负责授时和守时，并由可信的时间戳服务机构对电子数据摘要和权威时间记录进行数字签名生成时间戳。通过可信时间戳可确定电子文件生成的精确时间，并防止电子文件被篡改，为电子数据提供可信的时间证明和内容真实性、完整性证明，作为证据使用具有权威性和可信赖性，符合《电子签名法》要求，在法律上具备证明效力。

时间戳是不仅可以准确的标示出行为的发生时间，还可以通过时间的先后顺序构建可信的、完整的证据链条，是电子数据存证的

重要技术服务。

### （3）数据加解密

数据加解密是使用加密算法将明文数据转变为无法直接读取并理解的密文数据，拥有解密权限的人可以通过解密算法将密文恢复为明文数据。数据加解密应用在数据的传输、存储环节，保证数据在传输、存储中的安全性。加解密也是电子数据存证系统对于数据隐私保护的重要支撑。

### （4）数据存储

区块链链上通常为了控制数据传输量，只记录原始数据的哈希值，以达到电子数据保全的目的。还需对在区块链上固化的电子数据原文进行安全存储。数据存储系统使用安全的存储方式，同时拥有数据高并发、动态扩容等能力。

### （5）智能合约

智能合约以代码的方式实现既定的复杂业务逻辑，智能合约由合约参与方共同制定和维护，一旦部署则自动执行。智能合约具有自动执行的特性，可降低人为干扰和人工成本。智能合约技术为区块链用于复杂业务场景，支持垂直行业业务提供了支撑。

## （二） 区块链电子数据存证在司法实践中的应用价值

对于传统取证方式表现出成本高、效率低、真实性难以保证等不足。区块链技术适合作为一个电子数据存证的补充，区块链时间戳标示出电子数据发生时间，用户的私钥对数据的签名是用户真实

意愿的表达，区块链不易篡改、可追溯的特点方便对电子数据的提取和认定。证据在司法实践中的存证、取证、示证、质证等过程对应着电子数据的存储、提取、出示、质询等动作流程。

## 1. 区块链在电子数据存储中的应用

在电子证据生成时就可以将关键要素信息固定下来，通过区块链分布式、中心化无法修改的特性，可以保证在未来任意时间验证电子证据的原始性、完整性。

区块链系统具有难篡改、难抵赖、可追溯、系统稳定等技术特征：使用对等网络技术，每个节点都无差别储存一份数据，具有良好的崩溃容错；使用哈希嵌套的链式存储结构，保证每个区块的内容的更改都需要更改其所有后序区块，使系统数据安全，难以篡改；使用数字签名技术，对于每条数据都记录其出处，不可抵赖；使用合理的数据模型，使每条数据的流转都可以追溯到源起；使用时间戳技术，对于每条数据的生成时间有明确认定；使用内置智能合约，对于每类电子数据自动识别和处理，减少人为干预。

区块链电子数据存证，可以规范数据存证格式，保证数据存储安全，保证数据流转可追溯。

## 2. 区块链在电子数据提取中的应用

电子证据的取证过程有别于传统取证方式，是一个技术发现的过程。一般来说，在取证时不仅需要具有电子物证司法鉴定资质的机构和鉴定员来取证，还需要专业的律师共同进行，以保证技术的可

行性和取证的合法性。电子证据脆弱性、易变性等特征决定了其取证原件较困难，真实性难以保证。

因此，电子数据取证需要解决两个问题：一是如何获取电子数据原件；二是如何保证获取电子数据的真实性。

基于区块链的电子数据存证系统里的数据都经由参与节点共识，并且独立存储，互为备份，跑在符合要求的区块链电子数据存证系统中的数据均可通过技术手段认定为原件。账本具有难丢失难篡改的特性，记录了数据来源、数据时间戳、数据的流转过程等，可用于辅助电子数据的真实性认定。

### 3. 区块链在电子数据出示中的应用

目前电子证据的示证方式通常采用传统的书证形式，即将电子证据快照并进行纸质化。通过打印、公证等方式转换证据形式会增加当事人的时间、资金成本，阻碍诉讼效率的提升。转换成书证之后，电子证据的灵活性丧失，让丰富的证据形式变得单薄，缩小了当事人之间质证的空间。

基于区块链的电子数据存证示证可采用两种方式以降低示证过程的时间和人力成本，提高诉讼效率：一是可以采用智能合约自动取证示证和区块链浏览器示证的方法，采用自动化标准化的流程进行电子证据示证；二是可以通过将区块链存证、司法鉴定和公证电子证据出函流程打通，由多方参与示证。

#### 4. 区块链在电子证据质询中的应用

质证是指当事人、诉讼代理人及第三人在法庭的主持下，对当事人及第三人提出的证据就其真实性、合法性、关联性以及证明力的有无、大小予以说明和质辩的活动或过程。鉴于电子证据有别于传统证据的特点，审判人员在司法实践中对电子证据的真实性多持怀疑的态度，有时不得不转化为书面材料，甚至获得公证机关公证和司法鉴定机构鉴定。

电子信息的生成、传播、修改和储存都是以电子数据的方式进行的，书证化的电子证据其本质已经是复本。示证的间接性导致质证环节效率低。

基于区块链的电子数据存证系统因为优化了取证和示证环节，也让质证环节对于取证和示证的争议问题消除，聚焦于证据本身对案件的影响，提高了司法效率。

### 三、区块链存证提高电子证据认定效率

电子证据的认定是对电子证据“三性”的认定，本部分围绕电子证据的“三性”讨论区块链存证对证据“三性”的影响。区块链技术对电子证据“三性”的影响首先体现在对电子数据真实性判定有显著影响，其次区块链技术的相关技术、业务管理和链治理对电子数据的关联性和合法性也有部分提升。

#### （一）电子数据真实性认定的要素

由于电子数据存证的特殊性，其真实性可以从三个不同的层面



来认定：电子证据载体的真实性、电子数据的真实性和电子证据内容的真实性。

## 1. 电子证据载体的真实性

电子证据载体的真实性，是指存储电子数据的媒介、设备在诉讼过程中保持原始性、同一性、完整性，不存在被伪造、变造、替换、破坏等问题。电子证据载体的真实性，主要包括两方面的要求：一是电子证据载体来源的真实性。具体来说，法官审查电子证据时往往会关注：提交的电子证据是否包括原始存储介质，原始存储介质的收集程序、方式是否符合法律规定和有关规范；如果无法提取原始存储介质，如何确保其他存储介质能够保障电子数据的真实性。这是对电子证据载体原始性和同一性的审查。二是电子证据载体在诉讼前和诉讼中流转过程中的真实性。诉讼前和诉讼中，证据会在多个主体（如刑事案件的公、检、法和民事、行政案件中原被告、法院、被告）间流转。在此过程中需要考察：电子证据载体在移送、流转中是否保持同一性，是否符合鉴真的要求；电子证据载体是否保持完整性，没有被改变、破坏等。

需要明确的是，应当对电子证据载体的真实性和电子证据载体的原始性加以区分。由于很多电子证据是在网络、计算机系统中生成，导致无法判断认定哪台计算机、哪个存储设备是电子证据的原始载体。因此，在判断电子证据载体的真实性时，首先要审查是否存在电子证据的原始存储介质。如果能够确认，则通过原始存储介

质来认定电子证据载体的真实性；如果没有收集到原始存储介质，则需要通过技术措施、程序规则来确认电子证据载体的同一性。这意味着，电子证据载体的真实性和原始性并不相同，真实性的判断并不要求载体必须具备原始性。

区块链技术极大地扩展了电子证据的载体外延，并可以从技术上确保电子证据载体的真实性。具体而言，区块链存证使用分布式存储并附加防篡改校验机制，使电子证据可以脱离原始存储介质而安全存储，同时无被篡改之虞。

## 2. 电子数据的真实性

电子数据的真实性问题，是指作为电子证据信息在技术层面的存在形式的电子数据是否真实，是否与原始数据保持一致，是否存在被修改、删除、增加等问题。电子数据的真实性是电子证据内容保持原始性、同一性、完整性的技术前提，其对于电子证据真实性的审查判断具有基础性意义。

从法律规则来说，电子数据的真实性主要包括两方面要求：一是电子数据来源的原始性、同一性。由于电子数据存储于网络、服务器等介质之中，在诉讼过程中使用电子数据，必须进行提取，因此在提取环节应确保电子数据来源的原始性、同一性。二是电子数据在诉讼过程中保持同一性、完整性。在诉讼过程中，存储于介质内的电子数据会随着诉讼进程的发展而流转，因此应防止电子数据在流转过程中被修改、删除或者增加。

为保障电子数据的真实性，现行规范性文件确立了一些规则，其中既包括技术措施，也包括程序规则。例如，《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第二十二条第二项规定，对电子数据是否真实，应当审查“电子数据是否具有数字签名、数字证书等特殊标识”，这其实是对保障电子数据真实性的技术措施的审查。这些技术规则的适用，就是为了使电子数据在提取、使用过程中保持完整性、同一性。

电子数据的真实性，是区块链存证的真实性评价中的一个关键问题。因为，如前述，区块链技术可以保障电子证据的载体及载体上证据副本的真实性，但载体的真实和副本数据的真实，无法决定电子数据本身的真实性。同时，在区块链存证场景下，如果电子证据或其证据指纹（或称校验数据）上链并分布式存储，则证据的真实性已经具有技术保证。则欲保障电子数据的真实性，则需要确保作为电子证据的数据信息（或其证据指纹）在生成时即同步上链，或者确保该数据信息在上链前未被篡改。考虑到确保作为电子证据的数据信息在上链前未被更改实际上是一个传统的电子证据鉴定场景，不能发挥区块链技术的优势，故而在区块链存证领域，比较理想的确保电子数据真实性的方案即为作为电子证据的数据信息（或其证据指纹）在生成时即同步上链。

### 3. 电子证据内容的真实性

电子证据内容的真实性，是指：（1）在“排除合理怀疑”的证

明标准场合（如刑事案件特别是死刑案件中），电子证据所包含的信息可以与案件中其他证据所包含的信息能够相互印证，从而准确证明案件事实；（2）在“优势证据”证明标准场合（如民事案件中），电子证据所包含的信息可以证明一定的法律事实，特别是证明当事人的意思表示和法律行为。

电子证据内容的真实性是电子证据真实性的核心问题，不少语境中，电子证据的真实性，往往也是指电子证据内容的真实性。在司法实践中，鉴定意见、证据相互印证是确认电子证据内容真实性的主要方式，有些情况下二者还会同时使用。

当然，上链证据同非上链证据乃至非电子证据一样，也会在特定场景下面临证据内容和客观事实不一致的难题。

在区块链存证场合，证据载体的真实性和电子数据的真实性均得到区块链技术支撑、强化的背景下，电子证据的内容真实性有望得到一种“自我鉴真”的自证明效果。当然，在适用“排除合理怀疑”的证明标准的刑事案件中，使用区块链存证技术的电子证据如果系孤证，仍然要服从于“孤证不能定案”的原则，区块链存证不能等同于法律事实。而在适用“优势证据”证明标准的民事案件中，使用区块链存证技术的电子证据，一般可以逻辑推导出内容真实。比如，附加可信时间戳的上链数据，可以推定为形成于特定时间点，则该数据中的时间信息就具有内容真实性。同理，通过区块链达成的智能合约，在作为证据使用时可以推定合约内容数据真实，合约

内容数据也具有了内容真实性。

## （二）电子数据关联性和合法性的认定要素

### 1. 关联性认定

证据的关联性，是指证据必须和需要证明的案件事实或其他争议事实具有一定的联系。从证据法角度评价，关联性标准要求每一个具体的证据必须对证明案件事实具有实质性意义。换言之，一个证据的使用必须对证明案件事实或其他争议事实具有确实的帮助。故而，证据的关联性和证据的真实性未必有关。

区块链在单纯的存证场景应用，技术本身并不增强电子证据的关联性。如果是一类或一系列业务运行在区块链上，因其全流程留痕，可能因为可追溯性使证据的关联更加明确，方便进行关联性认定。

无论如何，上链证据和案件无关的情况不可避免，区块链存证不能确保电子证据具有关联性，而是在部分场景下为电子证据的关联性认定提供参考。

### 2. 合法性认定

证据的合法性认定包括取证主体合法性、证据形式的合法性、取证程序合法性以及证据保存与运用方式合法性四个方面。它是证据认定主体机械式对比法条的过程，其中不掺杂证据认定主体的私人价值评价。因此，与证据的真实性、关联性要求不同，证据的合法性判断不应考虑与案件事实的联系，而与法律规定密切相关。

### （三）区块链存证系统对电子数据认定的作用

区块链技术对电子数据证据认定的作用，即对电子证据“三性”的影响，首先在于对电子证据真实性的判定所产出的显著影响。此外，对于某些业务类型，诸如证据在链上形成并同步存储的情形，该系统对于证明所存证据的合法性和关联性也具有一定帮助。因此，区块链司法存证系统可以帮助司法工作人员，特别是法官和仲裁员，有效提高证据审查认定的效率和质量，降低审查难度和风险，对于提升案件质效和促进司法公正具有积极意义和重要价值。具体而言，该系统对于证据认定辅助功能主要通过以下四个层面来实现。

#### 1. 安全架构确保电子数据载体真实性

在系统架构层面，区块链共识机制协调参与节点记账并保证所有诚实节点的数据一致性。任何不超出共识范围的节点作伪，都可以被识别，避免了单点作恶的可能。同时不超出安全范围的节点崩溃，都不影响系统的正常运行，大大降低了崩溃丢失数据的可能。这种机制下，影响区块链系统的正常运行，需要有超过共识范围的节点数作伪或宕机（例如 33%），攻击成本极高。

区块链系统采用哈希嵌套的块链式存储结构。信息以交易的形式呈现，多笔交易打包成为一个区块，前序区块的哈希值嵌套进后序区块中。这种形式存储的数据，一旦某条数据被篡改，其后所有的数据都需要进行相应的修改，更改愈早存储的数据，其计算量愈大。

只有节点控制权具有足够的分散程度（分散程度是否足够取决于共识算法种类），存储的数据结构和哈希碰撞达到足够的难度，这种结构的优势和防篡改能力就会有足够的保障力度，就能够达到法律规定中关于能够有效地表现所载内容并可供随时调取查用，能够可靠地保证自最终形成时起，内容保持完整、未被更改（同时，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性）等要求，符合电子数据作为证据的法定标准。

## 2. 关键技术提高电子数据真实性

区块链司法存证系统除了区块链核心技术之外，还使用了其他关键技术，为证据认定提供了重要帮助。这些关键技术包括电子数据存储、可信时间戳、智能合约与虚拟机、隐私与数据加密等技术。

由于区块链本身上存储的只是哈希值，而非原件，因此在示证的时候如果没有原件与哈希值相对应，存证也将无法达到目的。因此，电子数据存储电子数据原件也是区块链司法存证系统的重要部分。

可信时间戳是将用户的电子数据信息和权威时间源绑定，由国家授时中心提供授时信息，将对电子数据信息和授时信息进行数字签名生成时间戳。通过可信时间戳可确定电子数据信息生成的精确时间，并防止电子文件被篡改，为电子数据提供可信的时间证明和内容真实性、完整性证明。

在区块链上，虚拟机是智能合约的运行环境，是一个可以完全对外隔离的完整计算机体系。区块链通过虚拟机来调用和执行智能合约，并要求所有节点都达成一致。通过在虚拟机执行智能合约，可以达成区块链上多节点之间计算结果的验证和一致，为在区块链司法存证系统中扩展更多的执行操作建立基础。

隐私与数据加密。区块链司法存证系统的节点和当事方并不希望自己的数据能够被其他无关的节点或者当事人自由的调阅。因此，基于数据加解密技术的隐私方案也是区块链司法存证系统的重要组成部分。

### 3. 相关技术提高证据认定效率

区块链司法存证系统除具备前述核心技术外，还融合了一些相关技术如：实名身份认证、关联证据追溯、操作行为审计、文件公示与送达、等辅助功能。这些辅助功能技术能够通过结合现有关键证据收储认定节点系统，来提升证据认定工作的处理效率并降低工作复杂度，一定程度上减免传统证据认定的非关键步骤。

实名身份认证。实名身份认证是网络安全法的强制性要求，也是区块链司法存证系统必不可少的重要环节。如果不进行实名认证，那么电子数据存证的签名无法追溯到法律主体，会对证据的真实性、关联性产生不良影响，影响证据的效力。相反，如果电子证据在存证时即是经过实名认证的数字签名进行签字确认，将大大减少质证过程中是否当事人本人签章的不必要验证甚至是签章鉴定活动，将



大大提高法庭质证效率。

关联证据追溯。在传统存证当中，共同制作的文件由于其文件的独立性，难以确认其关联关系，无法共同处理。但是在区块链司法存证系统中，多份共同制作的系列文件，可以通过关联证据追溯相关技术，确认证据之间的关联性，为法庭提供便利。

操作行为审计。在传统存证当中，谁接触并处理过证据原件，接触和处理的先后顺序是难以确定的；即使需要确定，也需要专业的鉴定机构介入。而使用操作行为审计相关技术，可以确定对原始数据的操作人、操作内容和操作顺序，为法官确定证据的效力和证明力提供证据支持。

#### 4. 相关业务和链下治理辅助证据认定

基于上述机制和技术特性，区块链存证系统还可以与公证、司法鉴定、审计等业务相互融合，彼此赋能，进一步提高所存储和输出证据的可信度。有效的链下治理如实名认证等，更方便对电子数据的合法性认定。运行在链上的业务形式，因系统可追溯以及可靠电子签名的特性，可能对电子数据的关联性认定提供帮助。

此外，由于在联盟链中，用户的授权和访问控制，需要由值得信任的管理员执行。建设方还需要选用满足条件的加密技术、可信的运行环境、保持节点的中立性等等。因此，还需要加强业务管理，完善联盟链治理，才能保证区块链存证系统在司法实践中真正有效发挥对认证环节的支撑促进功能。

## 四、区块链存证系统的参考架构

### （一）区块链存证系统的技术要求

#### 1. 合法合规性

合法合规是从电子数据的采集、存证发起方身份的合法合规性、取证方身份资质的合法合规性、存证运营主体的合法合规、节点是否可追溯、时间来源是否合法合规可核验、可否在法院电子证据平台进行多元证据追溯等方面进行定义，使得存储的电子数据能够作为司法证据进行采信，所以要从电子数据的内容及获取方式、存证发起人的身份信息、取证方身份资质、运营主体、节点、时间来源、验证方式进行规范：

##### （1）主体合法合规：

- 系统应对区块链节点运营主体有严格的评审，明确区块链节点运营主体的真实身份、联系方式等信息，保证区块链运营主体具有与服务规模相适应的技术人员及专业能力，并且有完善的管理机制。
- 系统应对存证发起人身份进行实名认证。
- 系统应做好发起人身份风险预警，对高风险用户的存证数据进行有效的预警和重点关注。

##### （2）过程合法合规：

- 系统对电子数据的生成、收集、传输过程应当符合相关法律法规的要求。

- 系统应有相应手段确定用户身份信息真实、意愿真实。

### （3）方式合法合规：

- 系统应使用公信力机构认证的取证工具，也可以通过从事电子数据检验鉴定机构的专职人员来进行规范化和制度化的取证，并保证证据获得的合法性。
- 系统应保证所存电子数据可以被验证与追溯，可以通过法院电子证据平台、司法鉴定机构或其他有司法效力的方式对证据进行追溯核验。

## 2. 数据强一致性

数据的强一致性是指区块链系统中各个节点存储的上链数据的一致性，进而达到数据可信共享的目的。数据上链之前必须先通过多方共识，避免数据不加校验的上链、避免数据在多节点的不一致，保证数据经过足够多节点的多方背书、多方签名再写入各个节点。每个节点在参与数据上链工作前，需检查自身落链区块的高度是不是最新，如果不是最新则需要先从其他节点进行区块数据同步后，方可参与数据上链共识。

区块链系统可以根据不同的业务需求，选择适用的共识算法来实现共识机制，但是都应遵从数据强一致性。共识机制功能组件应具备以下技术规范及功能：

- 系统应支持多个节点参与共识和确认。
- 系统应支持独立节点对区块链网络提交的相关信息进行有效性

验证，防止任意独立的记账节点未经其他记账节点确认而在区块链系统中进行信息记录或修改。

- 系统应具备一定的容错性，包括节点物理或网络故障的非恶意错误、节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误。
- 系统应采用统一可信的时间来源。

### 3. 便利性

简单、便捷、安全的访问、使用方式是用户使用的另一大需求，主要体现在接入、使用的便捷。

- 节点部署及组网的便利性：应该有便于各类机构部署节点，并且加入区块链网络的系统设计，可以在不影响现有区块链网络运行、不需新组织投入太大技术力量的情况下增加新的区块链上组织和节点。
- 开放接口的便利性：系统应设计易于调用、符合市场主流、兼容性强的接口，提供完善的接口文档，能够支持用户便捷地进行电子数据的写入、电子数据的查询、区块链信息的查询等。
- 区块链浏览器：为用户提供可靠的数据验证、数据操作溯源的功能，便于客户及时了解到真实的数据流转情况，也便于司法机构便捷的取到完整的证据链条。

### 4. 安全性

安全性是司法存证是否可以被法院采信的基础，在应用的各个

层面都有涉及，主要是系统的安全、数据的安全。系统安全包含：运行环境的安全、软件的安全、网络传输的安全。数据安全包含：数据存储安全、数据的不易篡改、数据的访问留痕、数据的隐私。

- 运行环境的安全：系统运行的依赖的硬件应当 7\*24 小时全天稳定运行，并且有完善的监控体系。系统存储应当有冗余备份，并且具有横向扩展的能力。
- 软件的安全：区块链网络以及应用系统都应该具有较强的安全能力，构建先进、主动的企业级安全威胁和漏洞检测体系，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。
- 网络传输的安全：网络传输过程应对数据采用业内通用的方式进行加密，并且能验证数据来源、数据完整性。
- 数据安全：机密数据应该加密存储，并且对密钥采用必要的保护机制；保证数据隐私保护，只有被授权方才可访问数据；通过可信联盟及相关技术以保证数据不易篡改、所有数据的访问留痕。建立智能、全面的监控审计体系，全方位监控数据的存储和流向，保障数据安全。

## （二）区块链存证系统的参考架构

区块链电子数据存证系统应用由参与方管理层、区块链层、应用层三个层级组成，其中电子数据存证系统由关键技术和应用服务两个子层级。

## 1. 参与方管理层

参与方以节点的方式加入区块链网络。司法机构节点、政务节点、企业节点、其他组织机构节点等共同参与组成电子数据存证联盟链，联盟链具有伸缩性，不同业务方可以根据需求加入和退出。参与节点之间信息互通，共同确保存证载体和存证数据的真实性。通过有效的制定统一适用的证据标准、证据规则、证据审查，从而有效的链接传递各个节点在不同案件中的身份职能与证据三性要素。

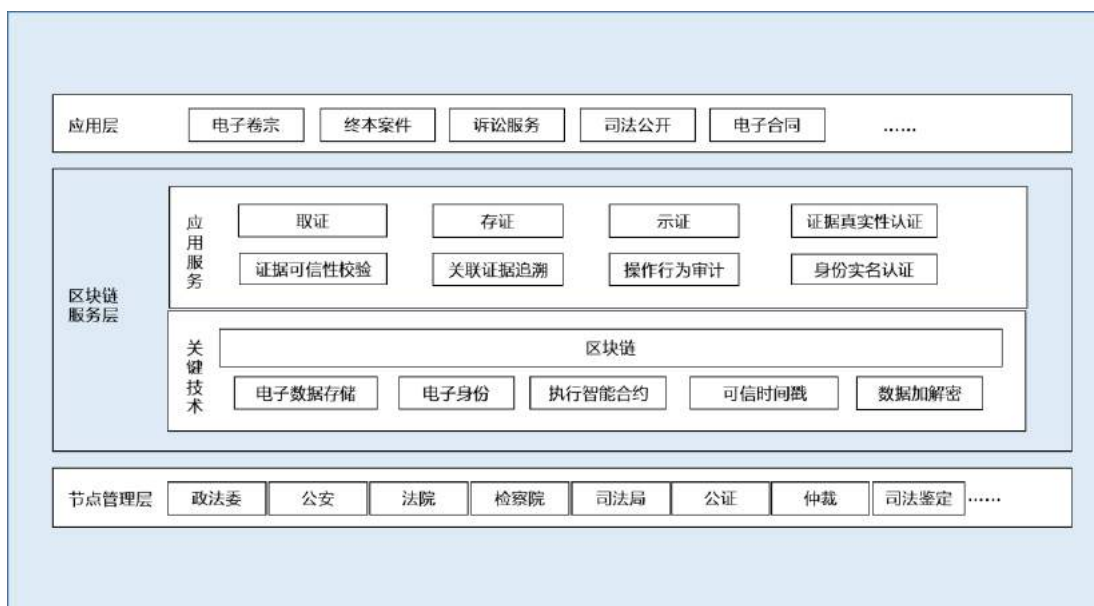


图1 区块链电子数据存证系统参考架构

## 2. 区块链层

### （1）关键技术

该部分是应用服务部分各模块的基础支撑。

#### a. 区块链技术

区块链技术，包括网络结构、数据结构、共识机制、签名验签等，是系统运行的基础。

## b. 区块链相关技术

数据存储模块。对在区块链上固化的电子数据原文进行安全存储。数据存储系统负责与底层存储介质进行交互，实现数据的高可用、灾备等能力；同时提供存储安全防护措施，避免数据被强行盗取；而数据存取审计，便于追溯电子数据变化和流转情况。

电子身份模块。对用户、设备进行区块链认证、登记标识其有效性，同时对用户的标识即私钥进行管理，该系统也包含访问安全功能，作为系统安全的重要保证。

时间戳服务。为系统提供统一时间服务。

执行智能合约。为系统以智能合约方式实现复杂业务逻辑提供安全执行环境，智能合约执行环境应高效、安全。

数据加解密模块。为系统提供数据加解密服务，该模块应支持国密算法，可支持可插拔的加解密算法。

## （2）应用服务

应用服务是在关键技术提供的支撑之上，针对各种服务模块进行实现和封装。该部分列举了电子数据存证全生命周期的相关服务。其中每个服务是由一组相关的规范、流程和配套的交互接口构成。服务中的规范和流程是依据司法行业相关规则 and 标准制定而成，以确保电子数据存证系统中固存的电子数据在司法行业应用中的质量和有效性。服务中的交互接口为司法行业专业系统高效、便利的使用本系统中的电子证据提供相应的支持。

### 3. 应用层

通过调用区块链层应用服务，经过二次开发对接特定业务场景。

## 五、区块链电子数据存证的应用场景

### （一） 法院行业应用

#### 1. 诉讼服务

应用区块链技术将诉讼服务过程中的电子材料、业务数据、用户行为等信息进行固证，防篡改、可验真、可追溯，确保诉讼服务数据的生产、存储、传播和使用全流程安全可信，提升电子诉讼服务的权威性、专业性和司法公信力。

将当事人进行网上立案、网上交费、网上开庭、证据交换等诉讼活动的登记信息、电子材料、操作行为全部上链，随时验真、追溯，提升网上电子诉讼服务的公信力和质效。

将诉讼服务过程中自动生成的送达地址确认书、庭审笔录、调解协议、送达回证、调查令等电子法律文书通过数字证书进行电子签名，确保身份真实有效，通过材料上链，实现材料固化和防篡改，保障在线电子生成法律文书的唯一性、真实性和法律效力，为诉讼全流程无纸化网上办理提供有力安全保障。

随着保险、银行、证券、电商等社会组织的数据上链固证，当纠纷产生时，可以构建基于区块链的涉诉单位、法院、鉴定机构等一体化纠纷办案平台，探索信用卡纠纷、金融借款纠纷等特定类型的一体化纠纷化解机制，一体化平台业务数据、电子合同等产生即



固化，线上直接提交给法院，实现全流程留痕、全节点见证、全链路可信，快速溯源、采信、利用，实现纠纷精准、专业、一体化快速化解，提升了诉讼服务效率和司法公信力。

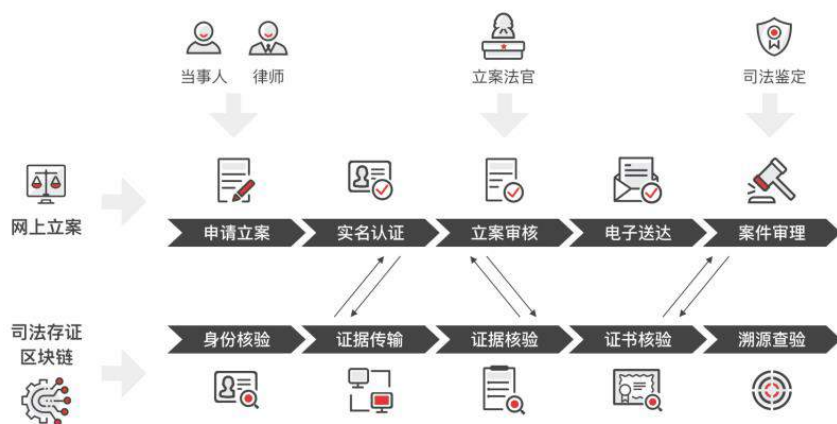


图2 诉讼中的证据流转示意图

## 2. 辅助审判

法官办案时查看当事人提交证据的上链情况，对存证证书、时间来源等进行查验追溯，辅助其证据认定，提升办案效率。同时，法官开展网上审理案件、网上阅卷等工作时，可将用户的行为、关键数据摘要、文书数据摘要、卷宗数据摘要等信息通过区块链技术节点上链，进行时间和哈希值的存证，可一定程度确保案件办理的公平公正。

## 3. 公示与送达

在传统存证当中，文件的公示与送达是难以确认，耗时费力的。但是在实名制支持的区块链司法存证系统中，文件是否进行了公示，当事人是否已经签收了文件，都是可以即时确认，无法抵赖的；这

一技术发展可能为法官节约大量工作时间。

#### 4. 辅助执行

应用区块链技术将执行案件办理过程中涉及到的财产查询、控制、处置等信息进行全流程记录，实现对财产处置流程的全程可追溯，确保执行案件对被执行人财产的查询、控制、处置流程规范可靠。

将执行案件中涉案款项的到账、发放信息及相关的电子材料进行上链固证，可防篡改、可追溯，确保每一个案件的每一笔款项来源、去向清晰可查，确保所有涉案款项流向全程可记录。

将执行案件中失信限高被执行人信息进行上链登记，可对失信限高被执行人的发布、撤销、屏蔽等行为进行全流程可追溯，确保将执行案件失信惩戒的威慑力发挥到最大作用。

将执行案件中线索悬赏任务、线索提交等材料及信息进行固证，可防篡改、可追溯，确保线索提交责任分明，保证线索悬赏对象明确。

应用区块链技术实现律师调查令的在线申请，并提供协助执行单位在线验证调查令真伪服务，确保律师合理合法利用律师调查令参与执行案件调查工作，充分调动律师参与案件财产调查的积极性，并确保调查行为合理合法、规范高效。

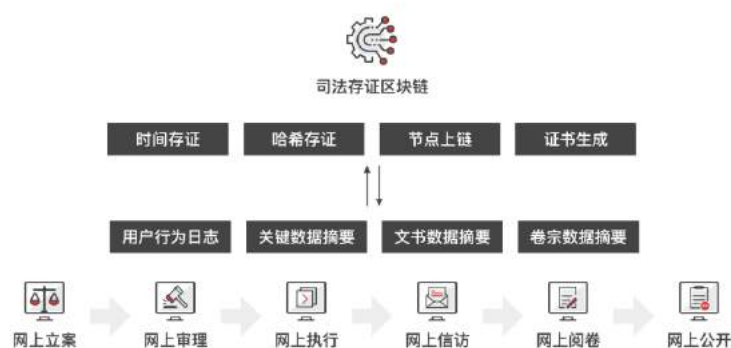


图 3 司法业务流程上链存证示意图

## （二）司法协同应用

基于区块链技术构建公安、检察院、法院、司法局等跨部门办案协同平台，各部门分别设立区块链节点，互相背书，实现跨部门批捕、公诉、减刑假释等案件业务数据、电子材料数据全流程上链固证，全流程流转留痕，保障数据全生命周期安全可信和防篡改，并提供验真及可视化数据分析服务。通过数据互认的高透明度，有效消除各方信任疑虑，加强联系协作，极大提升协同办案效率。

## （三）社会存证应用

### 1. 电子合同场景：

电子合同存证平台一个在去信任的环境下由多方共同维护的防篡改的分布式数据库。借助密码学的数学原理，可以确保数据在区块链上的防篡改与追溯。平台应提供在线签约（电子合同）+全业务流程存证“的一站式解决方案，在通过区块链实现合同的数字指纹信息分布式存储的同时，还可快速生成可信电子合同签署证据链，无缝对接和处理其中合同涉及的纠纷解决、仲裁机构裁决以及电子

证据递送等问题；而联盟参与方，如国内的司法鉴定机构，可以依托此存证联盟链，对鉴定中心保全的电子证据进行鉴定并出具鉴定报告。此外，针对商业环境以及客户需求，实现竞争公司之间的数据隔离需求，兼顾了参与各方的平等以及链上数据的隐私性，提高了数据在流转过程中的透明性和效率。

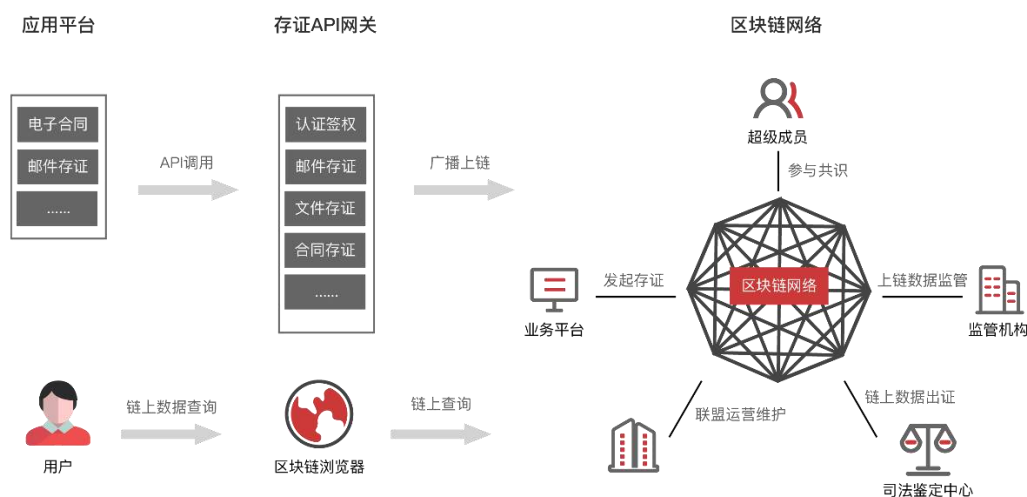


图 4 区块链电子合同平台示意图

## 2. 版权场景

### （1）侵权类取证

侵权类存证场景可以分为两类，第一类是侵权结果状态的取证，此时可对侵权的网页进行存证，对侵权行为的时间可查询可追溯。第二类是对侵权行为过程取证，属于动态的证据固化过程，需要有相关环境镜像系统进行配合，将证明过程通过可视化的方式展示出来，对时间段可查询可追溯可验证。



图 5 版权侵权取证示意图

- ✓ 当发现侵权行为时，快速调用版权服务中的侵权取证接口，对侵权网站进行页面抓取取证，并将取证结果保存在联盟链中；
- ✓ 系统对侵权URL地址进行域名解析，通过预言机服务将URL对应的侵权内容进行存储，并生成可供第三方检测的存证过程合理性证据，将侵权行为固化为证据进行保存；
- ✓ 固化后的证据保存在区块链中，数据永久存储且不可篡改，符合法律对电子证据的要求。

## （2）确权类存证

确权类存证场景分为以下两大方面：一是，知识产权权属证明，应用于版权证明、权利在先证明等领域，是对作品数据进行保护的行为，类似于著作权备案登记；二是，平台公告证明，或就发出过公告的行为以及对公告内容本身进行存证，对相关证据提取哈希、数字摘要并对时间进行固化。在进行确权类存证过程中，关键在于证明当事人在某一时刻完成了某内容或进行了某行为，且该时间及内容均不可篡改。

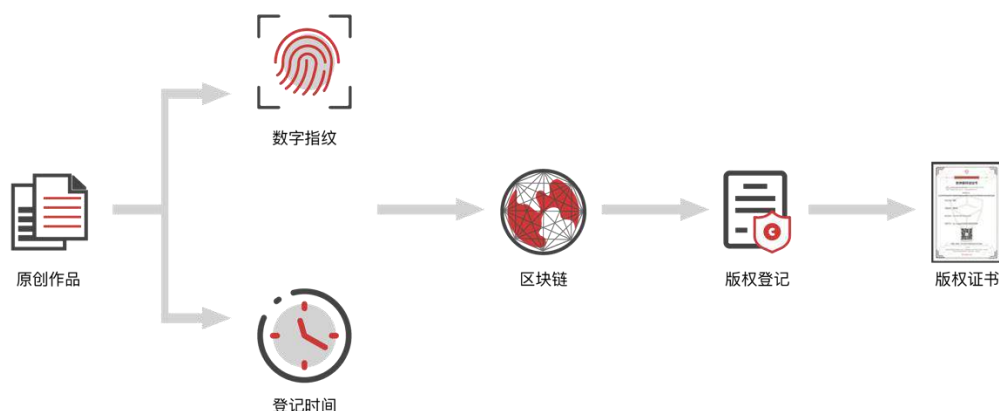


图 6 版权确权存证示意图

- ✓ 选择文件、获取数据指纹:选择需要存证的文件，通过哈希算法计算出该文件和关联信息的数据指纹。
- ✓ 数据写入区块链:在用户确认后，系统将得到的数据指纹写入区块链中，一经写入便无法篡改。
- ✓ 获取存证结果:根据用户需求生成存在证书供用户保留，也可根据用户需求，提供纸质书面报告。
- ✓ 数字指纹验证:根据客户需求，在用户需要对存证的指纹进行验证时，提供数字指纹比对查询。

### 3. 遗嘱存证

通过专业遗嘱见证系统，借助人脸识别、身份验证、密室登记、指纹扫描、现场影像、专业见证、文件存档、保密保管以及司法备案存证等功能，使立遗嘱人订立遗嘱的真实性得到了有力保障。涉及诉讼时，还将依法为当事人出具证明文件，遗嘱存证内容可在法院官方证据核验平台进行验证其真实性合法性有效性

- ✓ 对立遗嘱人通过人脸识别检测及指纹扫描等方式对其身份

信息进行验证。

✓ 有相关职业资质的人员经过授权后对立遗嘱人进行精神评估。

✓ 在密室进行全程同步录音录像，全程上链。

✓ 见证人签署保密协议，由两名以上工作人员对自书遗嘱内容全程见证。

✓ 遗嘱存证保全证书生成并可在法院官方证据核验平台进行查验追溯。

## 六、区块链司法存证存在的挑战

区块链司法存证的应用有光明的前景，但也存在一些挑战。司法领域因其权威性和强制性，存在一些特殊性，具体表现如下：

社会有多元化的司法生态需求，有效的立法支持能提高诉讼效率，然而法律的健全是相对的，不足是长期存在的。由于社会的发展，尤其是现在社会发展迅速，新事物、新现象不断出现，而法律从立项、到制定、发布往往需要相当长的时间，所以出现了法律与现实社会现象不同步、法律滞后等现象的产生。区块链作为一种新兴技术，从诞生至今刚满十年，电子证据应信息化普及而生，最多也不过几十年的历程，社会对于技术的认知尚未理性普及，法律层面的认定和定性还比较模糊，对于规范流程的各类规章制度都处于亟待补全的阶段。

传统模式下，证据的认定有其自有的一个模式，司法主体和各

参与方在此流程中已经成形各自的定位。无条款可依，使流程中各类主体固守本来业务范围，参与方之间难以进行定位和协调，也阻碍了业务模式的升级。

### **（一）法务与技术的对接不畅**

区块链技术目前处于时代前沿的新技术，从事区块链技术的工作者大都是 IT 行业一线的工程师，与法务工作结合点较少，对法务现状和痛点的了解不够深入，对司法这个特殊领域的合法合规要求认识不足。

司法工作由来已久，随着信息化的到来，电子证据的普及，一定程度上对传统司法证据系统造成了冲击，司法方开始有意识的引入新技术解决司法困境。但是法务工作的繁重让法务人员难以对技术市场有充分研究，对技术的深入探索就更加难以实现。

区块链技术与司法存证进行合法合规的匹配是区块链司法存证系统落地的一项挑战，对参与人员的技术水平和业务水准都有较高的要求，需要更多的通晓司法业务又了解区块链技术的复合型人才。

### **（二）区块链技术针对司法业务场景有待细化**

区块链技术自 2008 年出现以来，虽然保持着相当高的技术热度，部分区块链项目已经初步有了一些简单的应用场景，但整体而言，区块链技术还处于非常早期、快速发展的阶段。区块链依旧存在技术门槛较高、使用成本较高、代码容易出现安全漏洞等问题，不能完全胜任业务场景需求。



实实在在的应用场景是区块链技术良性发展的必要条件，然而司法业务天然具有业务逻辑复杂、业务情形多、业务容错率低等特征，这对应用的技术提出了更高的要求。区块链技术需要发展细化自身，针对司法业务场景，进行特定的模块化与合理封装，以便更适应司法存证的业务场景。

### **（三）电子证据司法认定规范有待明确**

传统业务模式下，对电子证据的认证非常困难，直接影响了审判中的采信比例。例如电子证据不同于传统物证，在证据法上都要求提交原件或者原物，而电子证据是以电子数据形式存储在电子介质之中的，传统的原件概念会对电子证据证明效力的实现造成障碍。示证中通常电子数据的展示方式是转化为书证，由于纸张的表现力所限，这种模式不但浪费资源，电子证据的多样性特征也无法表达。区块链系统出现后，因其存储的数据是多方共有多方维护的，中心化存证其数据原件的认定方式不再适用。区块链浏览器可以有效表现区块链系统中的数据存储，这种示证方式是否符合示证业务需求，暂无依据可循。因此，传统法务形式向新法务形式转变存在一定的挑战，业务模式上需要更新对证据的认识和制定适合电子证据的认证方法，若将电子证据仍置于传统证据的视角下，则无法有效缓解电子数据存证中存在的问题。

### **（四）民众接受程度有待提高**

虽然电子证据已经广泛存在，但是民众还没有充分的电子证据

意识，对于电子证据作为独立证据的司法效力没有确切的认识。区块链技术起源于 2008 年，技术和概念都比较新，区块链技术用于电子数据存证也是全新的尝试。因此基于区块链的电子数据司法存证，在民众电子证据意识的普及和民众对区块链电子存证系统的了解和接受程度上，存在一定的挑战。

## **七、结论**

### **（一）电子数据发展带来了挑战**

电子证据的出现给司法证明体系带来了巨大改变，随着证据多样化的激增，我们享受着信息化带来的便利的同时，也面对着新技术带来的巨大挑战。

电子证据伴随信息化而生，传统的电子证据采集和采信的过程中，常常遇到当事人意识淡薄、电子证据易湮灭、易篡改、管理成本高等痛点。导致司法服务面临巨大压力，难以满足日益增长的电子证据司法需求。尽管可信时间戳、电子签名等技术工具在解决电子证据的保全或真实性认定方面已经十分成熟，但在司法中的应用仍旧不普遍。

### **（二）区块链提升电子数据认定效率**

随着区块链的推广普及，越来越多的垂直行业从业方认识到区块链的价值并开始探索应用到自身业务中。电子证据的发展适应了信息化大潮，对于提升司法效率、降低司法成本有重要意义，区块链技术对于提升电子数据认定效率有使用价值。

区块链技术为电子数据存证提供结构化的采集过程，并借助于区块链技术不可篡改不可抵赖等优良特性，使电子数据的认定过程变得非常简便，解决电子证据在司法时间中易丢失、难认定的痛点，加快了电子证据的证据认定速度。因此得到了法院和社会各届越来越多的重视，很多有实力的厂商也纷纷在此领域进行尝试。信息时代，应强调电子证据的独特性质与内涵，改变对于电子证据不会用、不敢用、不能用的尴尬，从根本上推动电子证据制度的重构，真正让司法活动这一传统的社会化行为匹配人类进入信息化时代后的司法需求，让司法存证快速跨入信息化的时代。

### **（三）多参与方互通合作，完善标准推广应用**

公检法等多方以及技术供应商应协同一体，通力合作，完善标准、推广应用。

技术供应商作为技术的提供方和技术推动者，在保证技术稳定性的同时，应当积极拓展垂直行业应用场景。考虑技术的天然特征与传统业务场景的结合点，以技术促进业务模式变革和进步，加速技术服务于实体经济和社会民生。

在区块链司法存证领域，技术供应商应当积极普及技术理念，与业务方加强沟通，进行新业务模式试点，积极改造技术以适合业务场景，互取所需，合作共赢，为区块链这种新兴技术服务司法领域贡献一份力量。

我们应当充分认识到电子证据重要性，遵循客观规律，尊重电

子证据的本质属性，构建科学的电子证据规则体系，使得电子证据合法、合理、充分地被运用，实现电子证据应有的功能和作用。只有完善电子证据规则，电子证据的存证、取证、示证、质证、认证都有理可循，我们才能享受到电子证据带来的司法便利，迎来司法存证高效便捷的新局面。

## 参考文献：

- [1] 中国信息通信研究院.《区块链白皮书 2018》.
- [2] 王畅,范志勇.互联网金融案件中电子证据制度的适用[J].法律适用,2018(07):109-115.
- [3] 刘品新.印证与概率:电子证据的客观化采信[J].环球法律评论,2017,39(04):109-127.
- [4] 汪闽燕.电子证据的形成与真实性认定[J].法学,2017(06):183-192.
- [5] 樊崇义,李思远.论电子证据时代的到来[J].苏州大学学报(哲学社会科学版),2016,37(02):99-106.
- [6] 樊崇义,李思远.论我国刑事诉讼电子证据规则[J].证据科学,2015,23(05):517-530.
- [7] 孙波,孙玉芳,张相锋,梁彬.电子数据证据收集系统保护机制的研究与实现[J].电子学报,2004(08):1374-1380.
- [8] 褚福民.电子证据真实性的三个层面——以刑事诉讼为例的分析[J].法学研究,2018,40(04):121-138.

## 附件：参考应用案例

### 吉林省高级人民法院电子证据平台

吉林省高级人民法院区块链电子证据平台的构建，使案件证据的收集、核验以及存取更为安全、方便，实现了电子证据平台与电子法院的紧密配合。在准备提起诉讼之前或网上立案之后，当事人为了及时保护自己的合法权益，可以登录电子证据平台，进行证据的核验、存证、取证以及公示。在区块链电子证据平台完成证据相关的司法步骤之后，利用电子证据的取证便捷、公开透明以及不可篡改的优势，可在电子法院网上审判过程中直接对接电子证据平台的证据，完成电子法院网上证据交换与质证，促成纠纷的网上解决，提高司法效率。

网址：<http://evidence.e-court.gov.cn>

### 山东省高级人民法院电子证据平台

山东省高级人民法院电子证据平台可通过山东省高级人民法院官网首页进入，由山东省高级人民法院，中国科学院国家授时中心、中国信息协会法律分会、国家信息中心（中经网）、公安部第一研究所（中天峰）以及全国百家法院和中国司法大数据研究院等重要的区块链节点组成，并支持对接更多国家或社会组织的联盟链。

该平台支持证据核验、电子证据存证、电子证据取证、区块链公示等方面功能，重点解决互联网版权、互联网金融、电子合同等领域发生的纠纷类型。将互联网存证平台与法院建立区块链的数据

融合共享在案件审理与案件执行阶段，降低司法诉讼成本，提升解纷效率，防止数据篡改，推动诉讼服务及社会公信体系建设。

网址：<http://evidence.sdcourt.gov.cn/sdgy/#/index>

## 北京互联网法院“天平链”电子证据平台

“天平链”是北京互联网法院以“开放、中立、安全、可控”为建设原则，以通过主动式规则前置、司法全链条参与、社会机构共同背书、构建丰富应用为建设内容，以支持创新互联网审判模式为建设目标而进行建设的司法区块链。

自 2018 年 9 月 9 日“天平链”上线以来，完成跨链接入区块链节点 18 个，已完成版权、著作权、供应链金融、电子合同、第三方数据服务平台、互联网平台、银行、保险、互联网金融等 9 类 25 个应用节点数据对接。天平链在线证据采集数超过 472 万条，跨链存证数据量已达上千万条，案件审理中验证跨链存证数据 945 条，涉及案件 58 个。截至 2019 年 4 月 17 日，基于“天平链”认证判决案件 1 件，促成当事人和解的调解案件 41 件。

网址：<http://bc.bjinternetcourt.gov.cn:9999/tpl/>

## 杭州互联网法院“司法区块链”

2018 年 9 月 18 日，杭州互联网法院上线司法区块链平台。至今，该司法链已经汇集了 3.9 亿条的电子数据，相关案件调撤率达到 96% 以上。

杭州互联网法院在推动司法与区块链融合方面做了大量有益探

索并积累了丰富的实践经验。

2018 年 12 月，中国网络作家村上链司法区块链平台。通过司法区块链可以有效解决作者身份确定难、作品形成时间及内容固定难和侵权证据取证难等问题，帮助网络作家们足不出户、一键维权。

网址：<https://blockchain.netcourt.gov.cn/portal/main/domain/index.htm>

### **广州互联网法院“网通法链”**

广州互联网法院从顺应互联网产业发展需求出发，打造以审判为中心、以预防为抓手的可信电子证据存证平台——网通法链。

网通法链的建设以区块链技术为核心，通过密码学、共识算法、证据规则等要素的整合，建立了权威的多方数据存证模式。为确保数据的存储开放中立、安全可信，广州互联网法院与广州市中级人民法院、广州市人民检察院、广州市司法局、广州知识产权法院、广州铁路运输中级法院、中国广州仲裁委员会、广东省广州市南方公证处、广州公证处等 8 家单位共同组建司法区块链。

2019 年 3 月 30 日上线运营，日前网通法链存证的电子数据已经超过 545 万条。

### **郑州市中级人民法院电子证据平台**

郑州中院电子证据平台入口设在郑州法院诉讼服务网首页的电子证据版块，提供证据核验、电子存证、电子取证、区块链公示等服务。其中视听材料/电子证据包括电子合同等可以直接通过网页选择文件上传，电子数据的摘要也可实时入链。



该平台采用三层结构：一是区块链客户端程序，用户可以将操作行为如在线提交电子合同、维权过程、服务流程明细等通过程序全流程记录于区块链；二是区块链服务层，主要提供实名认证、电子签名，时间戳、数据存证等区块链全流程的可信服务；三是司法鉴定执行层，使用区块链技术将公证处、CA / RA 机构、司法鉴定中心以及法院作为节点连接在一起形成联盟链。

网址：<http://www.zzfysfw.gov.cn/zjy/>

### **成都市郫都区人民法院电子证据平台**

郫都区人民法院电子证据平台借助区块链技术，在电子证据存证取证环节，诉讼当事人可将电子合同提交、维权过程等行为全程记录于区块链，各机构节点进行全流程跟踪。

该平台可对证书内容与电子签名、当事人信息及哈希值等方面进行核验。打开当事人提交的“司法电子证据云《电子证据保全及认证证书》”（以下简称证书）对当事人身份进行验证，确认当事人已通过实名认证。通过多方证据核验平台，确认当事人提交的电子数据即为证书中所述电子数据，以此保证了电子数据的原始性。在多方证据核验平台的证书核验中对可信时间进行核验，在提交可信时间凭证编号与哈希值（数字指纹）验证后获得了“时间与事件对应关系明确，并且时间被认证是来源于国家标准时间，权威可靠、真实可信”的结果，以此确认当事人提交电子证据时间来源可信、可追溯、可查验。

网址：<http://pdfy.evidence.bjzjtp.com>

## 可信区块链推进计划

地址：北京市海淀区花园北路52号 邮政编码：100191

联系电话：010-62300249 传真：010-62304980

网址：[www.trustedblockchain.cn](http://www.trustedblockchain.cn)

